Cassandra Crossing 622/ Pannelli solari, aggiornamenti software ed armi cibernetiche

(622)—Il dubbio che l'Internet delle Cose possa essere usata come arma inizia a manifestarsi, ma si parla di minaccia hacker o...

Cassandra Crossing 622/ Pannelli solari, aggiornamenti software ed armi cibernetiche



Figure 1: AI-generated stock image by thenotetravel from https://www.123rf.com/

(622)—Il dubbio che l'Internet delle Cose possa essere usata come arma inizia a manifestarsi, ma si parla di minaccia hacker o potenziale aggressione cinese. Il vero problema non sono i "cattivi", ma piuttosto i modelli di sviluppo del software commerciale.

10 maggio 2025—Il recente blackout iberico non ha fatto esternare solo Cassandra; molti altri hanno cominciato a discutere tecnicamente dell'evento, ed i più previdenti anche di possibili eventi futuri, tanto più preoccupanti quanto più legati alla volontà di qualcuno.

Un esempio, che lega rete elettrica ed Internet delle Cose, è il vettore di attacco che utilizza i bug del firmware degli inverter degli impianti fotovoltaici per manipolare molti gigawatt di potenza elettrica installata, allo scopo di generare un collasso sistemico della rete elettrica, analogo a quanto successo poche settimane or sono nella penisola iberica.

Per chi non avesse voglia di leggersi questo articolo, ricorderemo che i pannelli solari generano corrente continua, mentre le reti elettriche trasportano corrente alternata.

Il device elettronico che permette ad un impianto fotovoltaico di connettersi alla rete elettrica e di mandarvi energia è appunto l'inverter. Suo è il compito di elevare la tensione della potenza elettrica generata dai pannelli fotovoltaici e trasformarla in corrente alternata, con la frequenza, e soprattutto la fase "giusta".

Forse l'ultima parola "fase" ha fatto arricciare il naso a qualcuno?
Per far si che la rete possa "accettare" la corrente di un generatore è necessario non solo che questa abbia la tensione e la frequenza giusta, ma anche che la fase sia esattamente quella della rete, come se rete ed inverter facessero pare di una squadra di nuoto sincronizzato.

Se un inverter, o qualunque altro generatore elettrico connesso ad una rete, "perde" la fase, o peggio ancora la frequenza, iniziano una serie di fenomeni energetici estremi, per cui è necessario disconnettere immediatamente i generatori dalla rete e fermarli, per salvaguardare l'integrità sia dei singoli generatori che della rete elettrica.

E' quello che è successo nel caso spagnolo; un singolo ed improvvido distacco di un collegamento in cui passava molta potenza elettrica ha richiesto alla rete elettrica una rapida e grande variazione di potenza, che ha fatto fluttuare frequenza e fase, ed ha prodotto una cascata di distacchi automatici e spegnimenti che si è estesa a tutti, dicasi tutti, i generatori della rete elettrica spagnola e portoghese.

Risultato? Tutto fermo, ed all'arrivo della sera tutto buio!

Ora il problema, la cui causa scatenante non è stata mai ufficialmente dichiarata, è molto preoccupante, sia che si tratti di un incidente che di un evento deliberato.

In ambedue i casi infatti, se questo fenomeno non fosse stato già noto a tutti gli eserciti dotati di forze ed armi cibernetiche, ora certamente lo è.

Ed il caso degli inverter degli impianti fotovoltaici, quasi tutti di produzione cinese e dotati di firmware largamente buggati, rappresenta un vettore di attacco alle reti elettriche così potente da arrivare oggi, in quanto tale, addirittura alla ribalta delle cronache.

Infatti, prendendo in maniera nascosta il controllo di un buon numero di inverter, si potrebbe realizzare facilmente un "pulsante rosso" con cui "spegnere" la rete elettrica di un paese nemico. Una ciberarma ed un piano di attacco tanto specifici quanto potenti.

Ottima sistema per danneggiare un paese nemico, sia in maniera "nascosta", sia mentre viene anche attaccato in maniera convenzionale.

Utile anche come arma tattica ad impiego circoscritto; ad esempio per avere una capitale al buio mentre atterrano le forze speciali incaricate di catturare il governo.

Non serve essere Sherlock Holmes per avere la certezza che i ciber-arsenali di molti paesi, se non lo possiedono già oggi, domattina avranno qualcosa di simile ad un tale bottone, e piani di attacco che ne prevedono l'utilizzo.

Ricordando la creazione e l'utilizzo della ciber-arma Stuxnet, operati da Stati Uniti ed Israele contro gli impianti di arricchimento isotopico dell'Iran, è un facile esercizio ipotizzare un piano cinese di destabilizzazione delle reti elettriche di altri paesi, già in atto per mezzo della vendita di inverter nel cui firmware fossero inseriti specifici bug o parti di software che ne permettessero il controllo "remoto".

Quindi cosa è necessario fare? Spegnere gli impianti fotovoltaici perché un tale ipotetico attacco potrebbe arrivare domattina? Impossibile per evidenti motivi.

Oppure bandire gli inverter cinesi, come già fatto per le celle 5G di Huawei, e sostituirli con "*onesti e sicuri inverter occidentali*"?

Difficile sia sul piano pratico che su quello commerciale ed internazionale; da chi e dove comprare centinaia di migliaia di inverter "sicuri" dall'oggi al domani, e chi finanzierebbe tutto il lavoro necessario?

Non è compito di Cassandra trovare una risposta, mentre certamente lo è vaticinare che **una risposta di questo tipo sarebbe errata sia tecnicamente che militarmente**.

Errata perché risolverebbe solo uno dei problemi informatici, uno dei vettori di attacco che possono **spegnere**, per sorte o per volontà di qualcuno, **una parte importante del delicato tessuto tecnologico che consente a nove miliardi di esseri umani di sopravvivere nella sottile superficie di questo pianeta**.

Errata perché il grande **problema che è necessario risolvere**, problema di origine esclusivamente antropica e finanziaria, **è quello del modello di sviluppo del software commerciale**, oggi applicato praticamente ovunque.

Questo modello, i cui dettagli non possono certamente essere esposti in poche righe, fa si che tutto il software prodotto oggi sia mediamente di qualità schifosa, sia dal punto di vista della qualità, che ancor di più della sicurezza.

In particolare il firmware, cioè il software installato negli oggetti "intelligenti", negli oggetti dell'Internet delle Cose, fa ancora più schifo della media, perché **essendo "*invisibile*" è considerato un semplice "*fattore di costo*" di altri prodotti, su cui spendere quindi il meno possibile.**

Non c'è da meravigliarsi quindi che anche il firmware degli inverter sia pieno di bug, e perciò facilmente utilizzabile come vettore di attacco.

E' necessario invece partire molto, ma molto a monte dei problemi contingenti degli inverter, e modificare il modello di sviluppo di tutti i firmware, oggetti impercettibili ma tuttavia vitali, per esempio irrigidendo le relative responsabilità legali civili e penali, rispetto a quelle in vigore oggi.

In questo auspicato processo, l'adozione estesa del modello di sviluppo del software libero ed open source dovrebbe essere uno dei tasselli principali.

I 24 impressionati lettori di Cassandra staranno in questo preciso momento pensando "*Ma allora non esistono soluzioni efficaci a breve o medio termine per risolvere questo problema degli impianti fotovoltaici, limitandone almeno le conseguenze sul piano di una guerra cibernetica.*"

Invece soluzioni di mitigazione a breve termine esistono, al punto che qualche decennio di esperienza lavorativa è bastata per far venire a Cassandra un'idea, peraltro già nota a chi del settore, e più ancora a chi di dovere. **Occuparsi prima di tutto degli aggiornamenti automatici dei firmware degli oggetti intelligenti**. E si, anche di quelli degli inverter fotovoltaici.

L'aggiornamento automatico del firmware, ormai dato per scontato come un fatto naturale della vita, rappresenta una ottima cosa per migliorare il il parco firmware installato che anima gli oggetti intelligenti, specialmente se i produttori fossero anche obbligati a farlo con regolarità e per tutta la vita di tali oggetti.

Ma rappresenta anche un potentissimo vettore di attacco multidimensionale. Un attaccante non avrebbe più bisogno di scoprire i bug di un firmware per costruirci un'arma cibernetica, e nemmeno di manipolare subdolamente per anni il firmware rilascio dai produttori.

Prendendo il controllo dei canali di aggiornamento del firmware, canali che sono quasi sempre dei colabrodo dal punto di vista della sicurezza, diventa semplice installare, velocemente, massicciamente ed al momento giusto, dei firmware manipolati che potrebbero disabilitare ogni oggetto intelligente, o trasformarlo in una ciber-arma “dormiente”, pronta ad essere risvegliata al momento opportuno.

Chi avesse dei dubbi si ricordi che, come per Stuxnet, **non stiamo parlando di ipotesi, stiamo raccontando la storia**. Lo dimostra il caso della disabilitazione dell’Internet Satellitare, avvenuto all'inizio della campagna russa contro l’Ucraina, proprio utilizzando un aggiornamento massiccio del firmware dei modem satellitari.

Ed affrontare questo non banale ma ben più semplice problema sarebbe un ottimo inizio per risolvere poi tutte le altre vulnerabilità delle reti tecnologiche, che le rendono suscettibili ad incidenti e vulnerabili ad attacchi informatici.

Nell'interesse di tutti.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica “Quattro chiacchiere con Cassandra”
Lo Slog (Static Blog) di Cassandra
L’archivio di Cassandra: scuola, formazione e pensiero

***Licenza d’utilizzo**: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link*.*

By Marco A. L. Calamari on May 20, 2025.

Canonical link

Exported from Medium on August 27, 2025.